TCIPG

Trustworthiness Enhancement Tools for SCADA Software and Platforms

Trusted Software Stack for Control Systems

Julian Bangert, Sergey Bratus, Rebecca Shapiro, and Sean W. Smith

GOALS

- Control systems can be served by policies and mechanisms considerably **more restrictive** of allowed computation than those of general-purpose systems. We aim to develop such mechanisms **throughout all layers** of a control system.
- We aim to develop **concise** policies that capture programmers' **intent** at every architectural layer of a control system without burdening the programmers with additional policy tasks (as in, e.g., SELinux).
- We aim to capture **intent-level semantics** in control applications, standard libraries, kernels, and network- and bus drivers, for maximal reduction in unintended (malicious or exploitable) computation.
- We aim to keep all of our mechanisms **lightweight** & **maintainable**.

FUNDAMENTAL QUESTIONS/CHALLENGES

- General-purpose programming platforms and SCADA platforms hugely differ w.r.t. computation they should allow. The former must be flexible to support development of programming models; the latter should **restrict any computation not explicitly intended** by developers.
- SCADA systems are increasingly built on **commodity** general-purpose platforms, for cost and development flexibility reasons.
- General-purpose systems include legacy but no longer necessary optimizations embedded in their tool chains, which make extra room for attacks. For example, both Linux and Windows **discard semantic information** present in binaries and libraries when creating processes.
- Solutions limiting unintended computation must be **compatible** with the platform's Application Binary Interface (ABI) or **retrofittable** to it.
- Restricting unintended computation must be done on **every architectural layer** of a control system, to prevent the "squishy" vulnerability mass from migrating to an unmitigated layer.

RESEARCH PLAN

Stack of Trust: A Multi-Layered Protection Strategy

Trust Stack Level	Our Solution
Process-Level Mediation	**ELFBac:** Instrumentation system for binary programs that allows users to isolate and secure pieces of a binary without needing to rewrite the original program. **STATUS:** In development. Looking for collaborators!
System Call Mediation	**Behavior-Based Policy:** Policy languages that clearly identify trustworthy behaviors, and use techniques such as context-dependent goals and isolation primitives to enforce the policy. **STATUS:** In development. Looking for collaborators!
Kernel Host Intrusion Detection Systems	**Autoscopy Jr.:** An intrusion detection system that lives within the OS kernel itself, monitoring for control-flow anomalies while imposing minimal overhead. **STATUS:** Complete.
Hardened Kernel	**grsecurity/PaX*:** A set of Kernel hardening patches that include additional OS protection mechanisms. **STATUS:** See * note below table.
Custom Trapping Scheme	**FlexTrap:** A system that allows for variable-sized caching in the Translation Lookaside Buffer (TLB) of a system, letting users define their memory accesses to be as coarse or granular as needed. **STATUS:** In development. Looking for collaborators!
Kernel Drivers	**CrossingGuard:** An application of traditional IP network defenses to the USB interface. **STATUS:** In development. Looking for collaborators!
Network Hardware	**Predictive YASIR:** A low-latency message authentication system that tries to predict the plaintext content of messages and pre-send the ciphertext before receiving the entire message. **STATUS:** Complete.

(*) Note that grsecurity/PaX is © Open Source Security, Inc., and is not a Dartmouth product, but rather a set of patches that are freely available from http://grsecurity.net

RESEARCH RESULTS

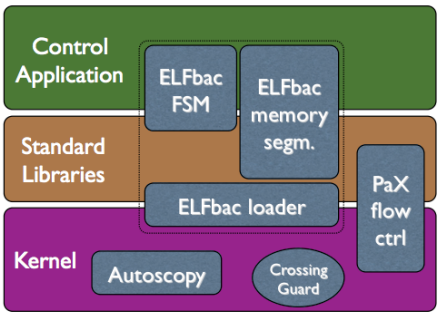
- Network hardware-level effort has been completed, with prototype technology tested and transferred.
- Lightweight kernel intrusion detection research and a prototype have been completed and informed the design and implementation of a secure control system at an industry partner.
- A prototype port of the PaX tehcnology has been completed and awaits testing in conjunction with other components (tested with Autoscopy).
- The ELFbac kernel component is in beta-stage testing. The design has been described in Dartmouth Technical Report **TR2013-727, ELFbac: Using the Loader Format for Intent-Level Semantics and Fine-Grained Protection** (Julian Bangert, Sergey Bratus, Rebecca Shapiro, Michael E. Locasto, Jason Reeves, Sean W. Smith, and Anna Shubina), which has already received significant exposure in the security industry and is being adapted into a conference publication.
- CrossingGuard is in development; preliminary results have been published at the Workshop on Embedded Systems Security (WESS) and are featured on a separate poster.

BROADER IMPACT

- Many non-SCADA systems share the challenges of control systems, e.g., medical systems and other cyber-physical systems. Although built on general-purpose platforms for ease of development and testing, they are meant to be restricted to a narrow set of computations once deployed. Our work will benefit designers of such systems.
- Trustworthiness of computer systems is predicated on our ability to mediate events that can lead to compromise on every level on which the system's control logic and data flows are changeable (especially when changeable because of attacker manipulations). By taking a computational approach to trustworthiness, we defeat classes of manipulation techniques, not just particular bugs or exploits.

INTERACTION WITH OTHER PROJECTS

- The following chart depicts the interaction components of the stack:



FUTURE EFFORTS

- We will continue development of the ELFbac programming model, the policies, and their compositional tools.
- We will coordinate with the grsecurity/PaX team to produce a stronger hardening variant of their protective schemes.
- We will investigate the use of compiler plugin technologies for suppressing unintended data and control flows, both in the kernel and in control applications.

FUNDING SUPPORT PROVIDED BY DOE-OE AND DHS S&T